Review Session

Ennan Zhai
ennan.zhai@yale.edu
Today’s Mission

• USENET & Gossip
• Firewall & NATs
• Cryptographic tools
• Reputation
• Unstructured search
• Structured search
Today’s Mission

- USENET & Gossip
- Firewall & NATs
- Cryptographic tools
- Reputation
- Unstructured search
- Structured search
USENET & Gossip

- USENET format (RFC1036)
- Gossip protocol
  - Rumor-mongering;
  - Anti-entropy;
  - Security problem.
USENET & Gossip

- USENET format (RFC1036)
- Gossip protocol
  - Rumor-mongering;
  - Anti-entropy;
  - Security problem.
If Alice reads a message locally on her machine containing the above headers, what can you infer is the name of Alice’s machine?
If Alice reads a message locally on her machine containing the above headers, what can you infer is the name of Alice’s machine?
If Alice reads a message locally on her machine containing the above headers, what can you infer is the name of Alice’s machine?

**cbosgd**
Alice sends a private message to Jerry’s USENET post, but Jerry did not receive it. After several days, Alice sees some new posts from Jerry with a Path: header line of ‘cbosgd!mhuxj!ucbvax!eagle!jerry’.

What do you expect happened to Alice’s original message to Jerry?
Alice sends a private message to Jerry’s USENET post, but Jerry did not receive it. After several days, Alice sees some new posts from Jerry with a Path: header line of ‘cbosgd!mhuxj!mhuxt!eagle!jerry’.

What do you expect happened to Alice’s original message to Jerry?
Alice sends a private message to Jerry’s USENET post, but Jerry did not receive it. After several days, Alice sees some new posts from Jerry with a Path: header line of `cbosgd!mhuxj!mhuxt!eagle!jerry`.

What do you expect happened to Alice’s original message to Jerry?
USENET & Gossip

- USENET format (RFC1036)
- Gossip protocol
  - Rumor-mongering;
  - Anti-entropy;
  - Security problem.
USENET & Gossip

If you are operating a malicious peerster in our lab and you want to achieve an evil target, how do you do that?
Today’s Mission

- USENET & Gossip
- Firewall & NATs
- Cryptographic tools
- Reputation
- Unstructured search
- Structured search
Firewalls & NATs

- NATs:
  - IP address.
- Firewall:
  - How it works;
  - Defending against bad guys or good guys?
  - Design.
Firewalls & NATs

- **NATs:**
  - IP address.

- **Firewall:**
  - How it works;
  - Defending against bad guys or good guys?
  - Design.
Firewalls & NATs
Firewalls & NATs

Session A → S
dst: 9.9.9.9:9999
src: 5.5.5.5:5555

(desired P2P session)

Server S
9.9.9.9:9999

Client A
10.1.1.1:1111

Client B
10.2.2.2:2222
Firewalls & NATs

Diagram showing a network setup with NAT (Network Address Translation) and firewall configurations.
Firewalls & NATs

- NATs:
  - IP address.

- Firewall:
  - How it works;
  - Defending against bad guys or good guys?
  - Design.
set ffilter src-ip [ip-address] dst-ip [ip-address] icmp-protocol
Firewalls & NATs

set ffilter src-ip 192.168.2.2 dst-ip 61.172.201.194 icmp-protocol

set ffilter src-ip 61.172.201.194 dst-ip 172.27.20.240 icmp-protocol
set ffilter src-ip 192.168.2.2 dst-ip 61.172.201.194 icmp-protocol
set ffilter src-ip 61.172.201.194 dst-ip 192.168.2.2 icmp-protocol
Today’s Mission

- USENET & Gossip
- Firewall & NATs
- Cryptographic tools
- Reputation
- Unstructured search
- Structured search
Cryptographic Tools

• Public/private key encryption/signature
• Diffie-Hellman key exchange
• Hash function
Cryptographic Tools

Alice uploads a file “foo.txt” to the Internet and computes MD5 value for the file. After a few days, Alice downloads the file but finds the file is not the one she uploaded. Interestingly, the MD5 value is the same. What happened? How we can deal with this situation?
Today’s Mission

- USENET & Gossip
- Firewall & NATs
- Cryptographic tools
  - Reputation
- Unstructured search
- Structured search
Reputation Systems

• Peer-based reputation systems:
• Object-based reputation systems:
  - Computing the reputation scores
  - Potential attacks
Reputation Systems

Voter 1 +1
Voter 3 +1
Voter 2 -1

File 1
Reputation Systems

similarity?

Voter 1

Voter 3

File 1

Voter 2
Reputation Systems

Reputation?

File 1

Voter 1

Voter 3

Voter 2
Today’s Mission

- USENET & Gossip
- Firewall & NATs
- Cryptographic tools
- Reputation
  - Unstructured search
- Structured search
Unstructured Search

- Flooding
- Random walk
- More
Unstructured Search

Running algorithm A. What's the traffic?
Today’s Mission

- USENET & Gossip
- Firewall & NATs
- Cryptographic tools
- Reputation
- Unstructured search
- Structured search
Structured Search

- Chord
  - The algorithm;
  - Complexity.
- Attacks
Structured Search

Three objects:
1, 2, and 6
Structured Search

Three objects: 1, 2, and 6
Structured Search

Three objects: 1, 2, and 6
Structured Search

Three objects: 1, 2, and 6
Structured Search
Structured Search
Structured Search
Structured Search

![Structured Search Diagram]

The diagram illustrates a structured search algorithm, likely related to distributed systems or database indexing. The circular structure with nodes labeled 0 to 7 represents a ring or a distributed network. Each node contains a finger table with start, interval, and successor information, and a 'keys' section indicating the keys stored or managed by each node.
Structured Search
Question 2 in Example
Question 2 in Example

\[ R(u) = \sum_{c,t: \exists P(u,c,t) \ u \neq u} \sum |P(u_i, c, t)| \]

where, \( P(u_i, c, t) \) represents the set of postings by consumer \( u_i \) that annotates content \( c \) with tag \( t \); \( |P(\ldots)| \) denotes the size of the set \( P \).
Question 2 in Example

\[ R(u) = \sum_{c,t: \exists P(u,c,t)} \sum_{u_i \neq u} |P(u_i, c, t)| \]

where, \( P(u_i, c, t) \) represents the set of postings by consumer \( u_i \) that annotates content \( c \) with tag \( t \); \( |P(\ldots)| \) denotes the size of the set \( P \).

<table>
<thead>
<tr>
<th>user</th>
<th>content item</th>
<th>tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>c1</td>
<td>a</td>
</tr>
<tr>
<td>2</td>
<td>c1</td>
<td>a</td>
</tr>
<tr>
<td>3</td>
<td>c1</td>
<td>b</td>
</tr>
<tr>
<td>4</td>
<td>c1</td>
<td>b</td>
</tr>
<tr>
<td>5</td>
<td>c1</td>
<td>b</td>
</tr>
<tr>
<td>3</td>
<td>c2</td>
<td>a</td>
</tr>
<tr>
<td>3</td>
<td>c2</td>
<td>c</td>
</tr>
<tr>
<td>4</td>
<td>c2</td>
<td>c</td>
</tr>
</tbody>
</table>
Question 2 in Example

\[ \text{rank}(c, t) = \frac{\sum \forall u \in \text{users}(c, t) R(u)}{R_0} \]